Windows 2000 Security Architecture

Peter Brundrett
Program Manager
Windows Security Team
Microsoft Corporation

Session Prerequisites

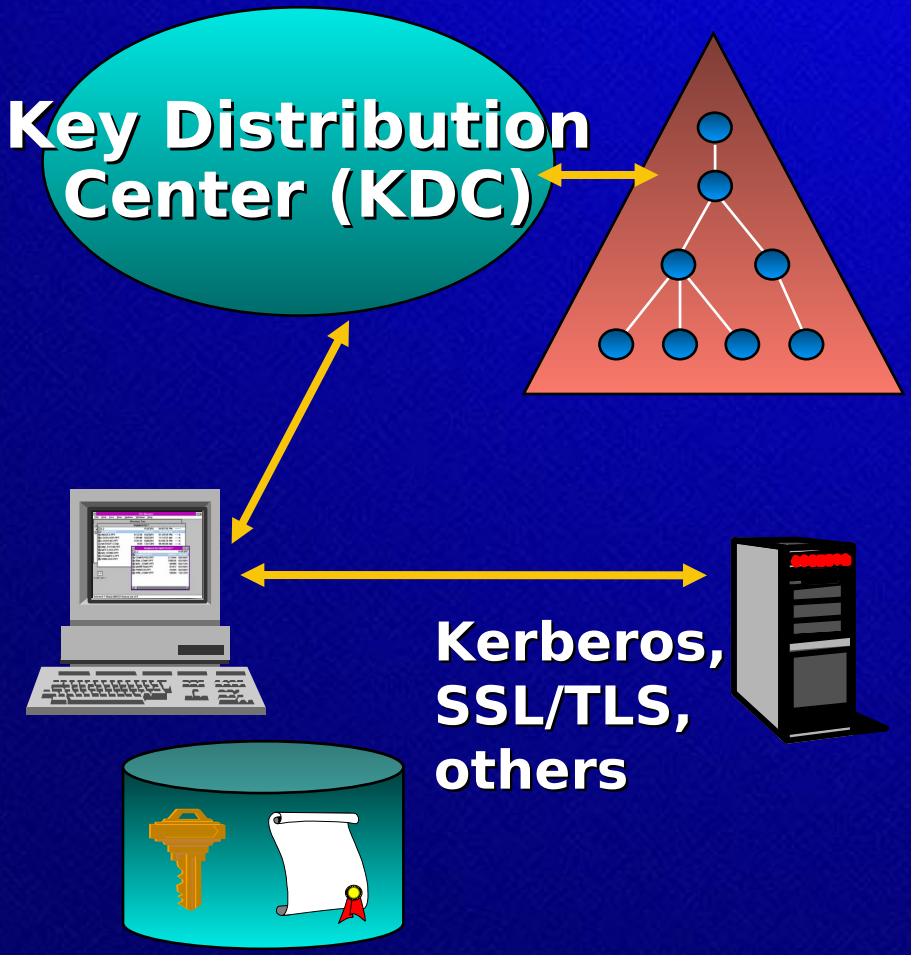
- This session provides an overview of Windows 2000 Security
  - Assumes you already know about Windows NT 4.0 security
  - No security protocol details
  - No cryptography
  - We will look at system design
- This is a level 300 session

Topics

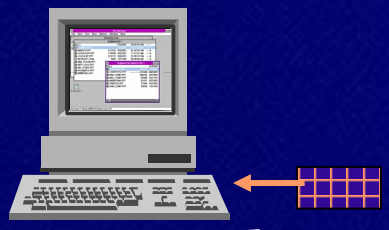
- Enterprise single sign on
- Kerberos V5 integration
- Security provider architecture
- Public key security components
- Encrypting file system
- Network data protection
- Security policy

Windows 2000 Single Sign On

- Single account store in Active Directory
- Integrated Kerberos v5 logon
- Protected store for public key credentials
- Industry standard network security protocols



Smart Card Logon



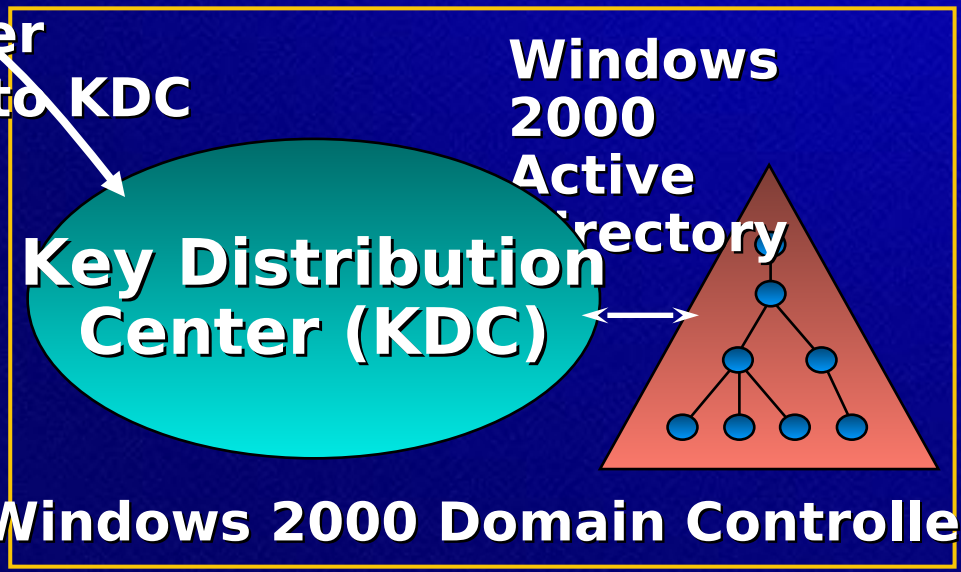
TGT

1. Insert smart card to reader, activate card with PIN

2. Private key and certificate on card authenticates user to KDC

3. KDC returns TGT response protected by User's public key certificate

4. Account control option requiring smart card logon per user



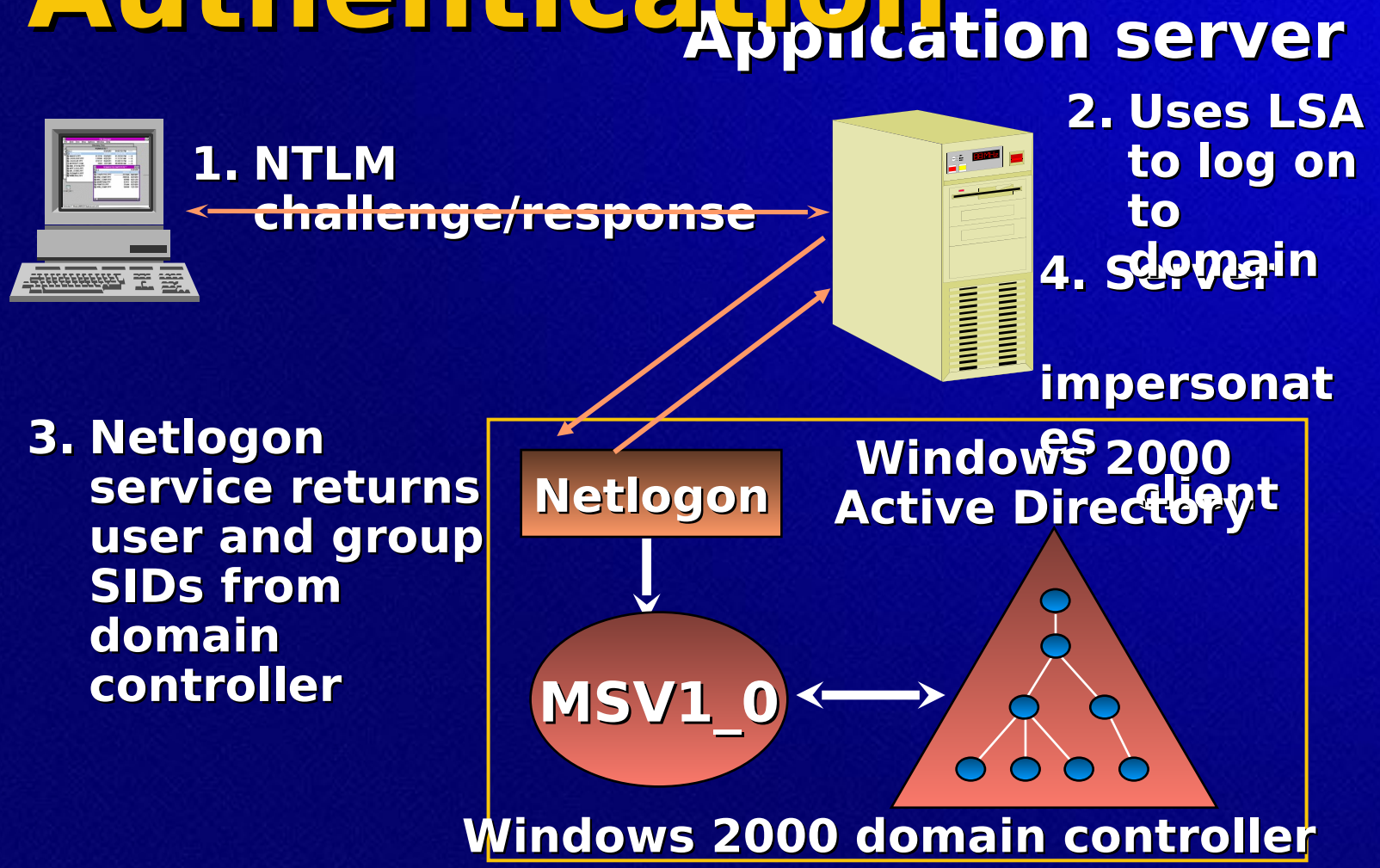
Authentication and Authorization

- Authenticate using domain credentials
  - User account defined in Active Directory
- Authorization based on group membership
  - Centralize management of access rights
- Distributed security tied to the Windows NT Security Model
  - Network services use impersonation
  - Object-based access control lists

One Security Model: Multiple Security Protocols

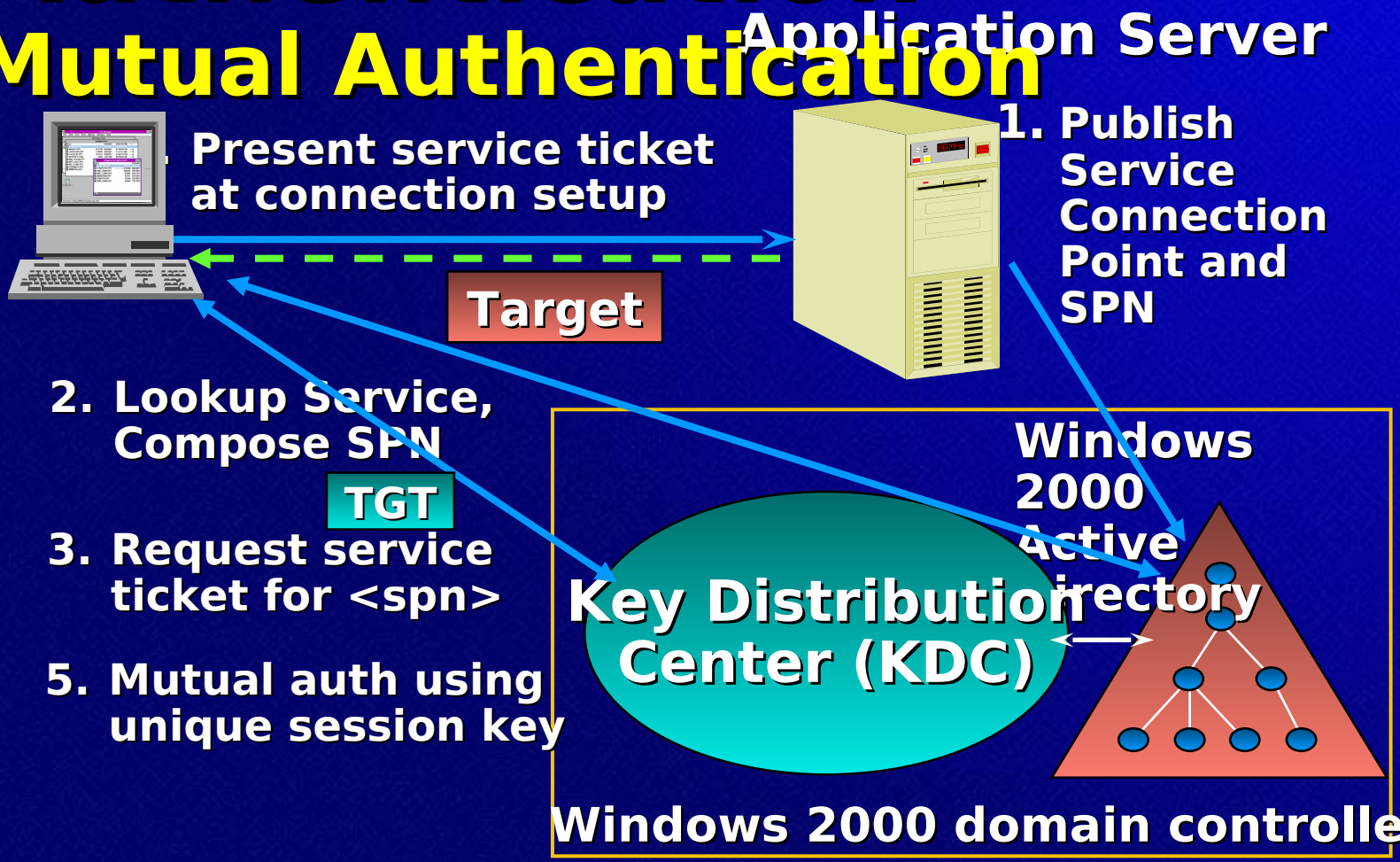
- Shared key protocols
  - Windows NTLM authentication
    - Compatibility in mixed domains
  - Kerberos V5 for Enterprise networks
- Public key certificate protocols
  - Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
- Multiple forms of credentials in the Active Directory

NTLM Authentication



Kerberos Authentication

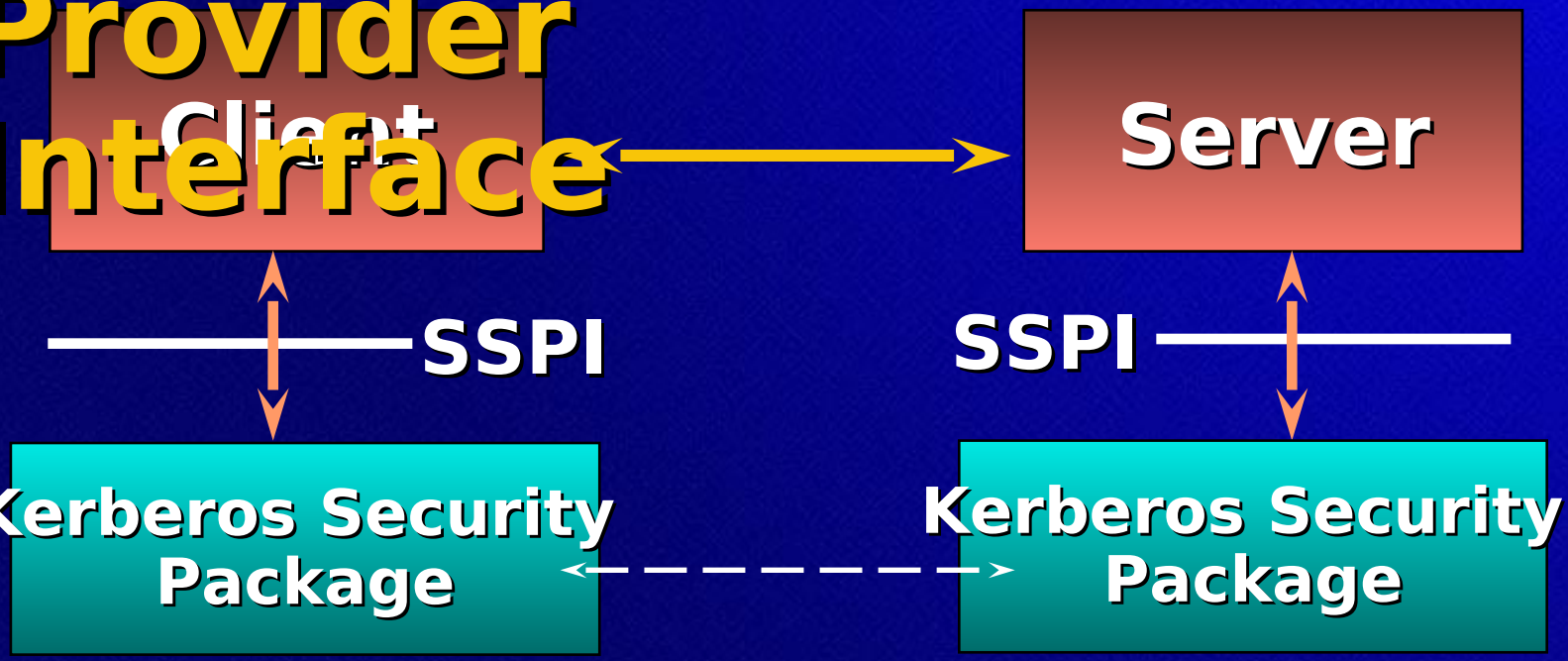
Mutual Authentication



Kerberos Protocol Advantages

- Faster connection authentication
  - Server scalability for high-volume connections
  - Reuse session tickets from cache
- Mutual authentication of both client, server
- Delegation of authentication
  - Impersonation in three-tier client/server architectures
- Transitive trust between domains
  - Simplify inter-domain trust management
- Mature IETF standard for interoperability
  - Testing with MIT Kerberos V5 Release

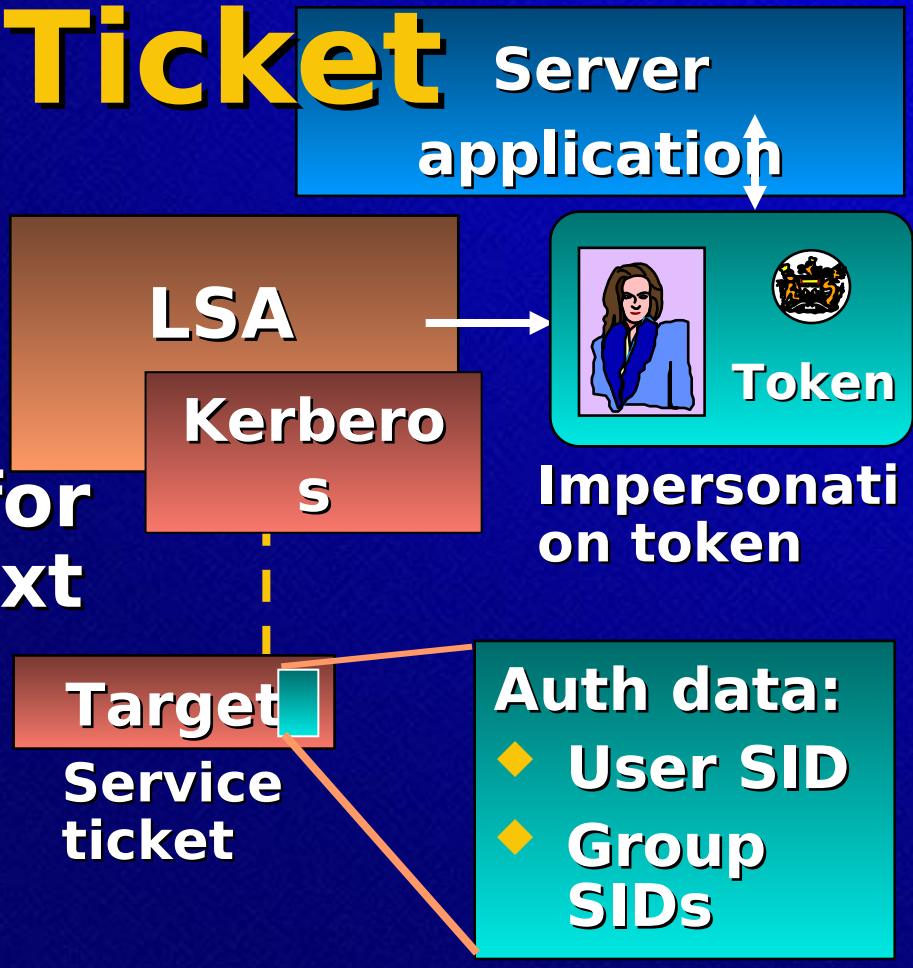
Security Support Provider Interface



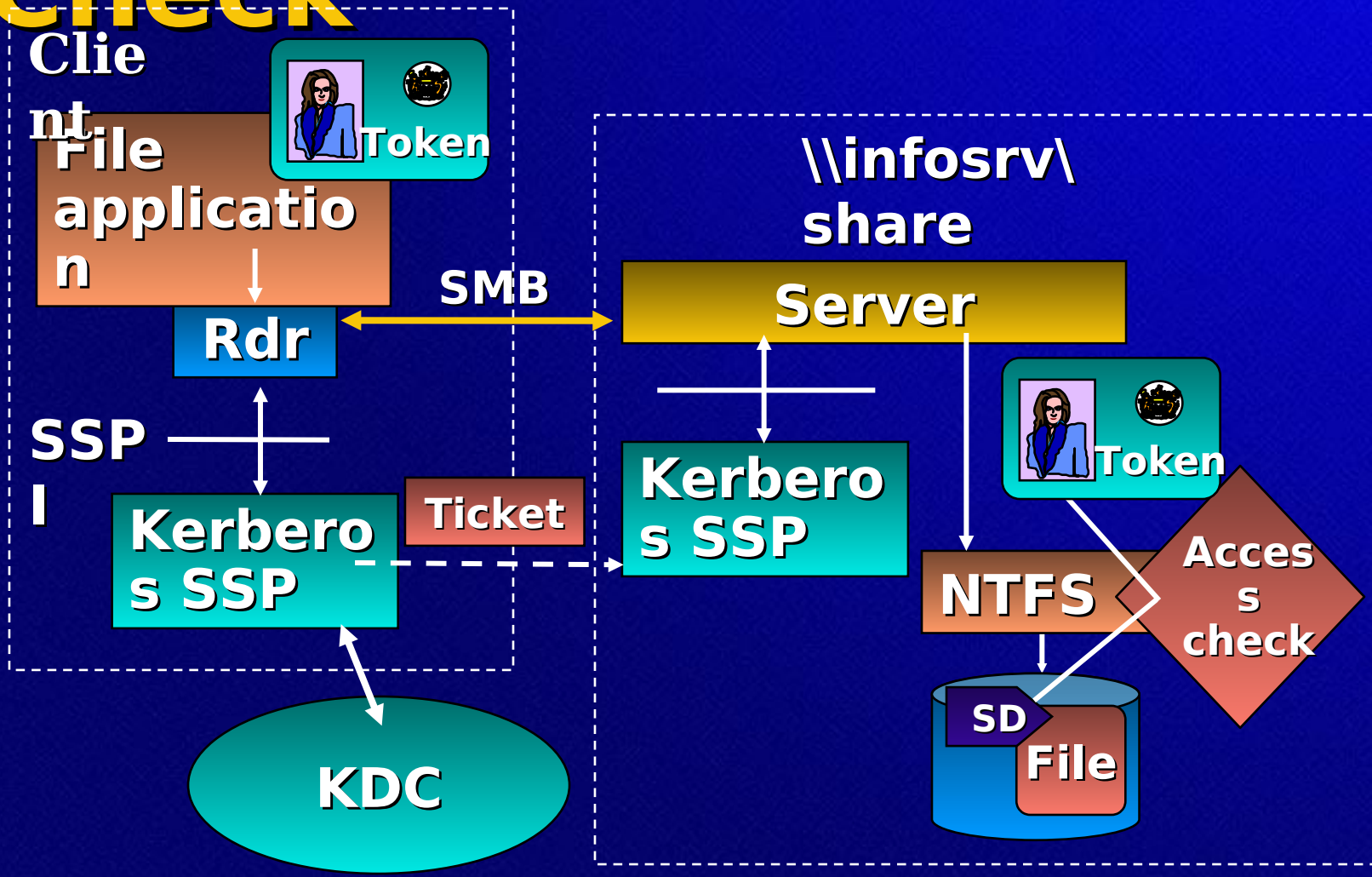
- Application protocol carries all data
- Kerberos SSP manages security context

Building An Access Token From A Kerberos Ticket

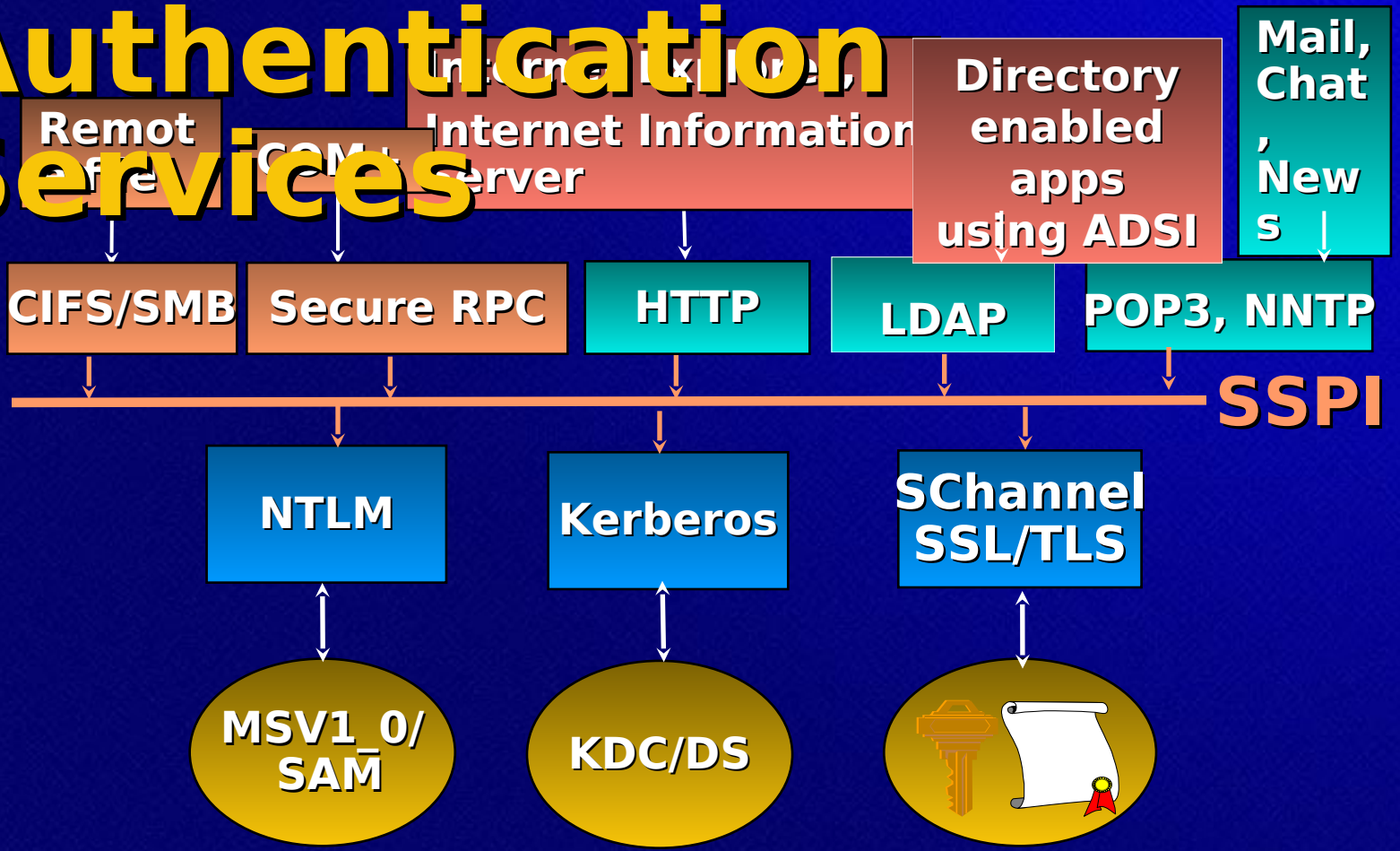
- Kerberos package gets auth data from service ticket
- LSA builds access token for security context
- Server thread impersonates client context



Remote File Access Check



Architecture For Multiple Authentication Services



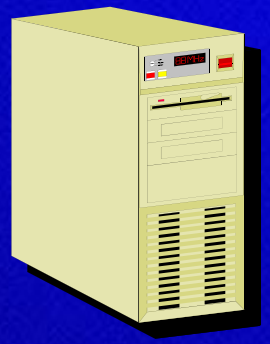
Public Key Components

For clients

- User key and certificate mgmt
- Secure channel
- Secure storage
- Auto enrollment
- Trust policy

For servers

- Key and certificate management
- Secure channel
- Client authentication
- Auto enrollment

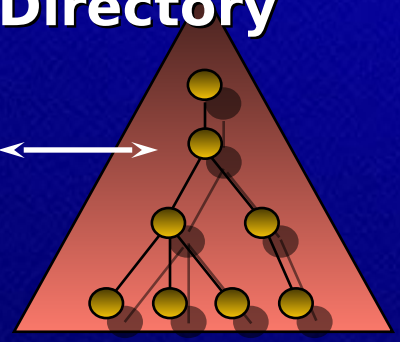


Enterprise

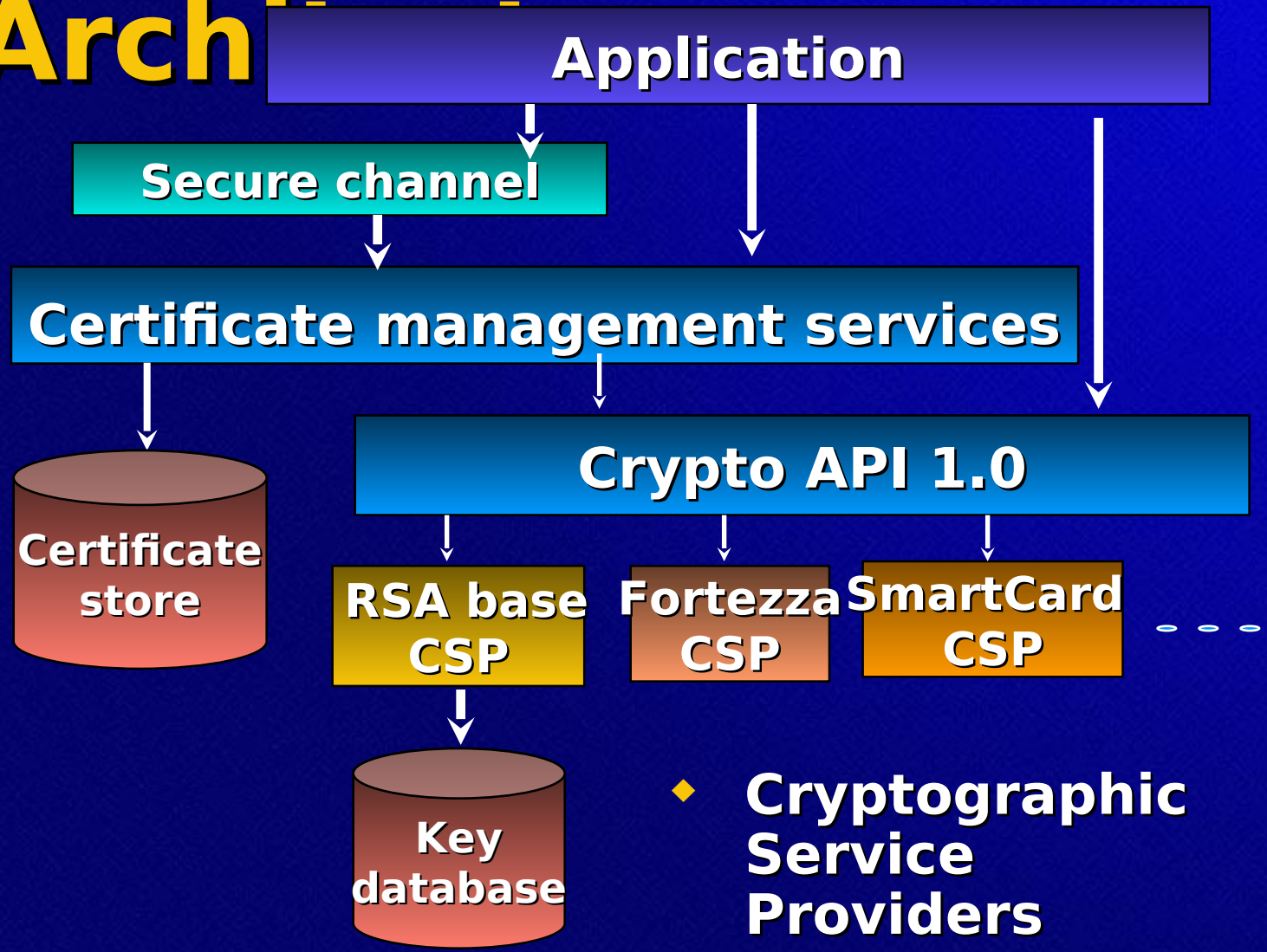
- Certificate services

Windows 2000 Active Directory

Certificate Services



Crypto API Architecture

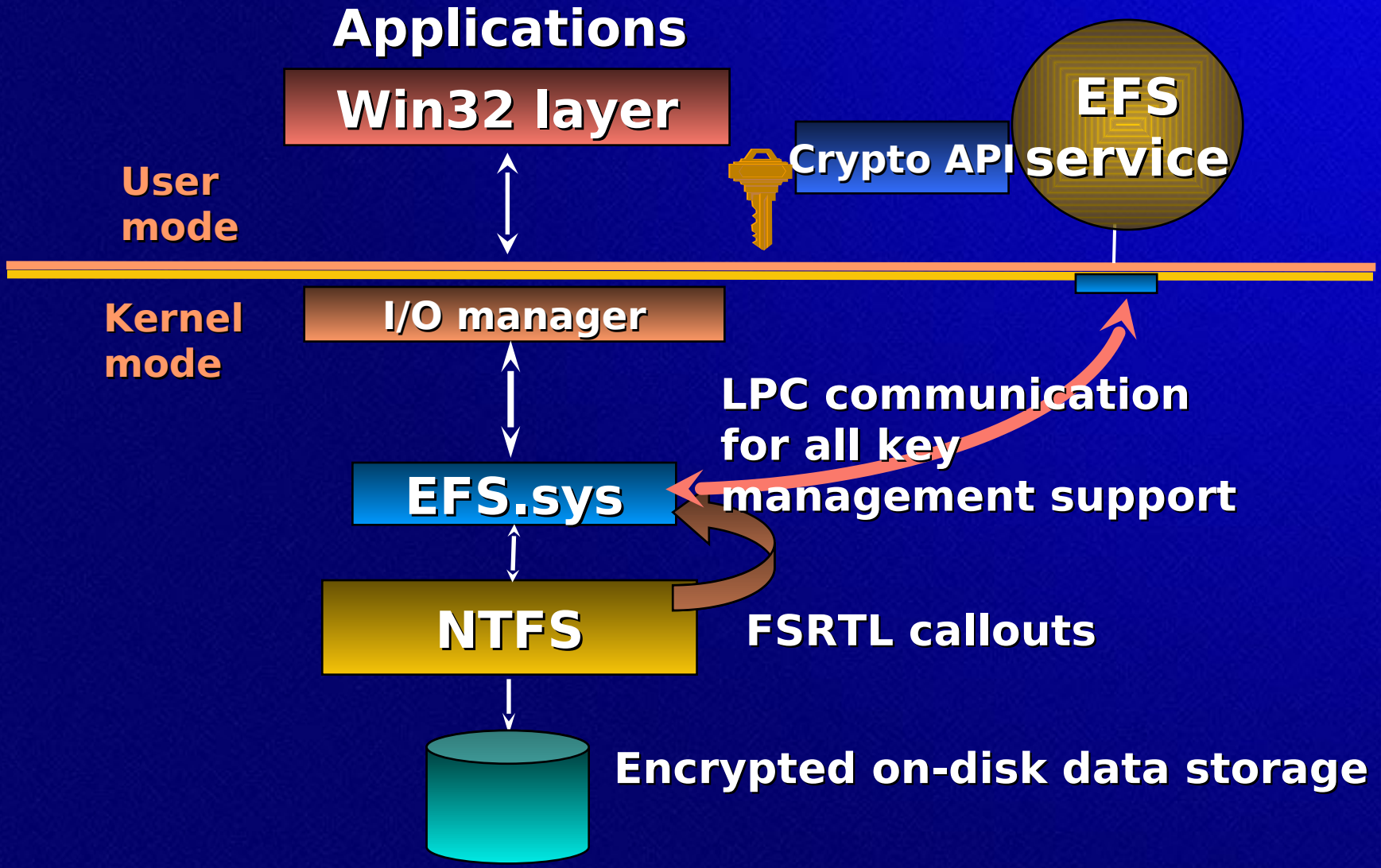


- Cryptographic Service Providers

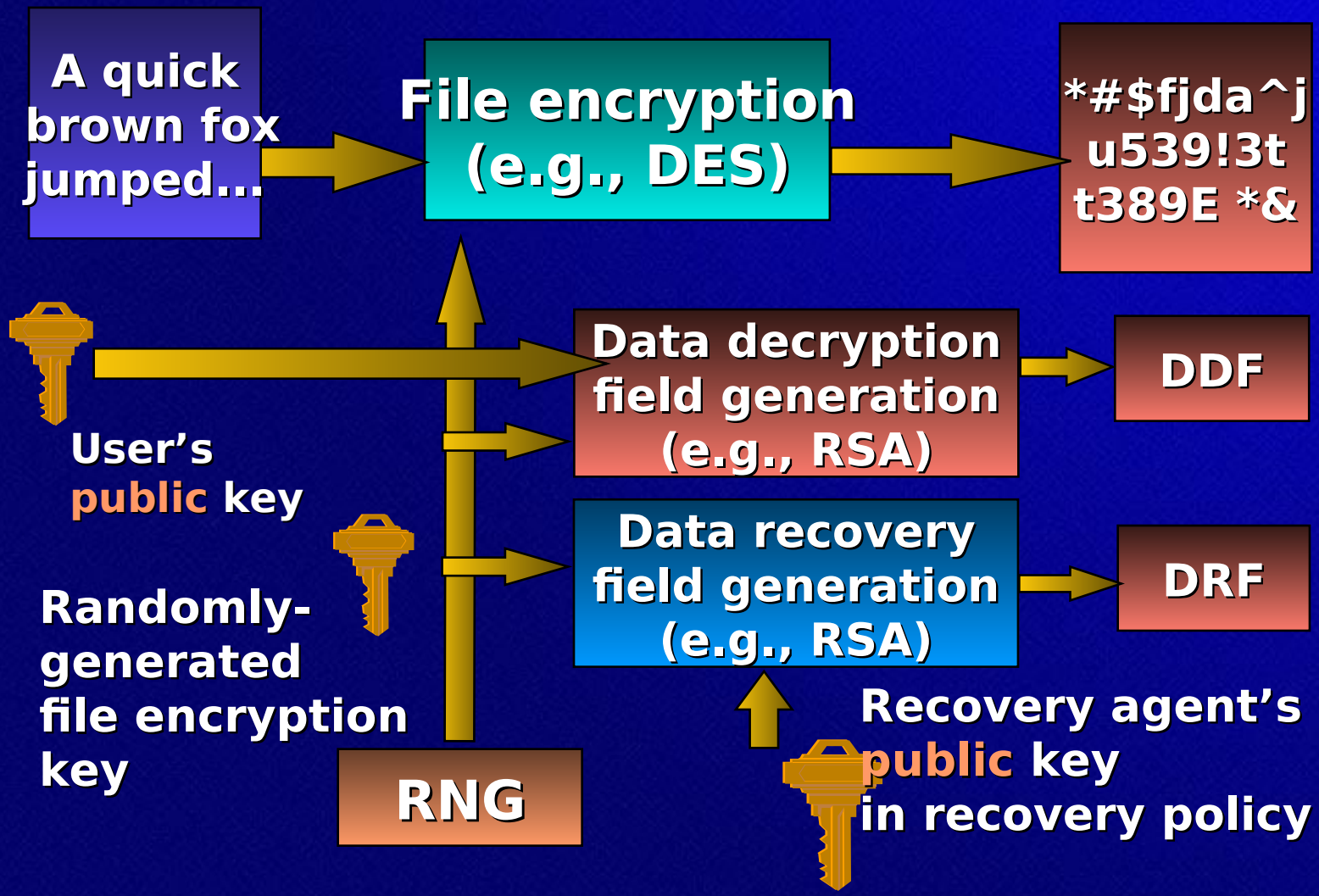
Encrypting File System

- Privacy of data that goes beyond access control
  - Protect confidential data on laptops
  - Configurable approach to data recovery
- Integrated with core operating system components
  - Windows NT File System - NTFS
  - Crypto API key management
  - LSA security policy
- Transparent and very high

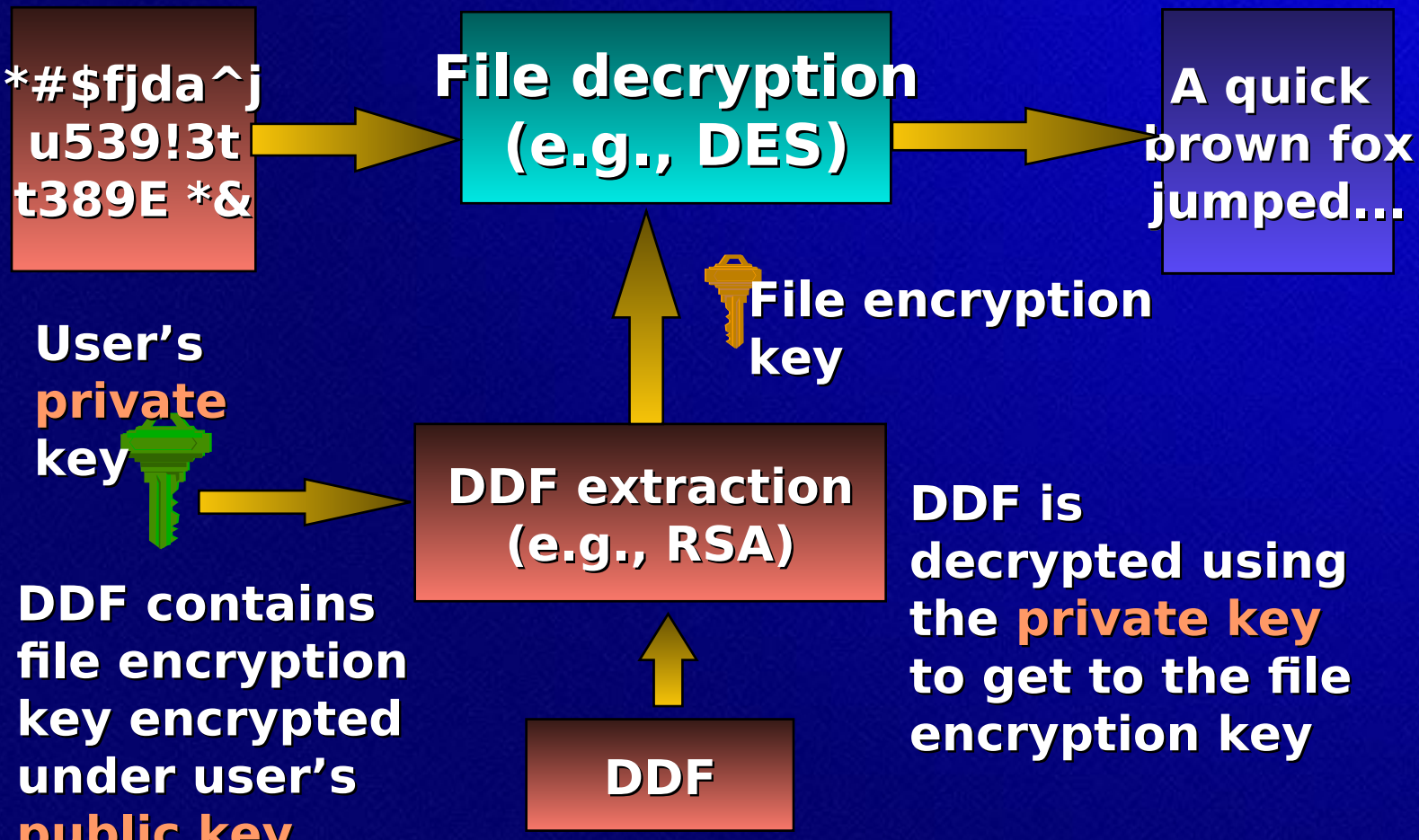
EFS Architecture



File Encryption



File Decryption

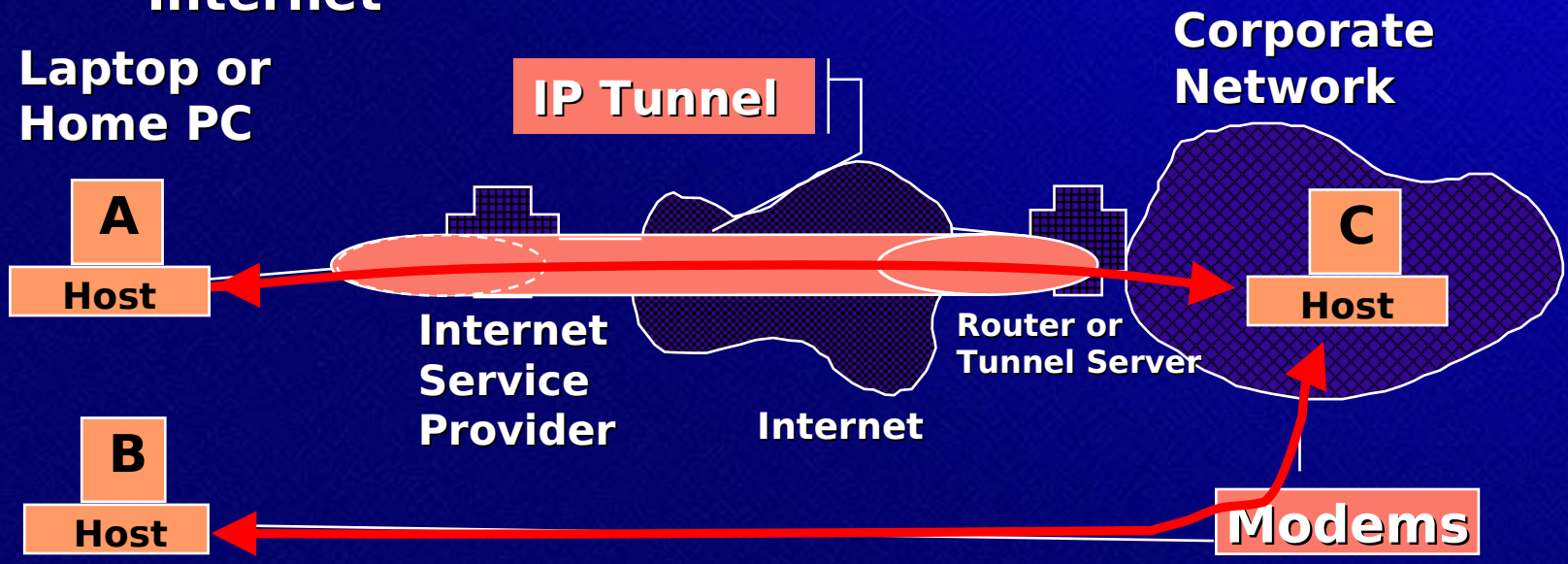


Secure Networking

- Internet Protocol Security (IPSec)
  - ISAKMP/Oakley - IKE
- Extended Authentication Protocol/PPP
  - SmartCard support – EAP/TLS
  - Token – EAP/SDI
- Remote Authentication Dial In User Service (RADIUS)
- Kerberos security package
- Public key (SSL/TLS) security package

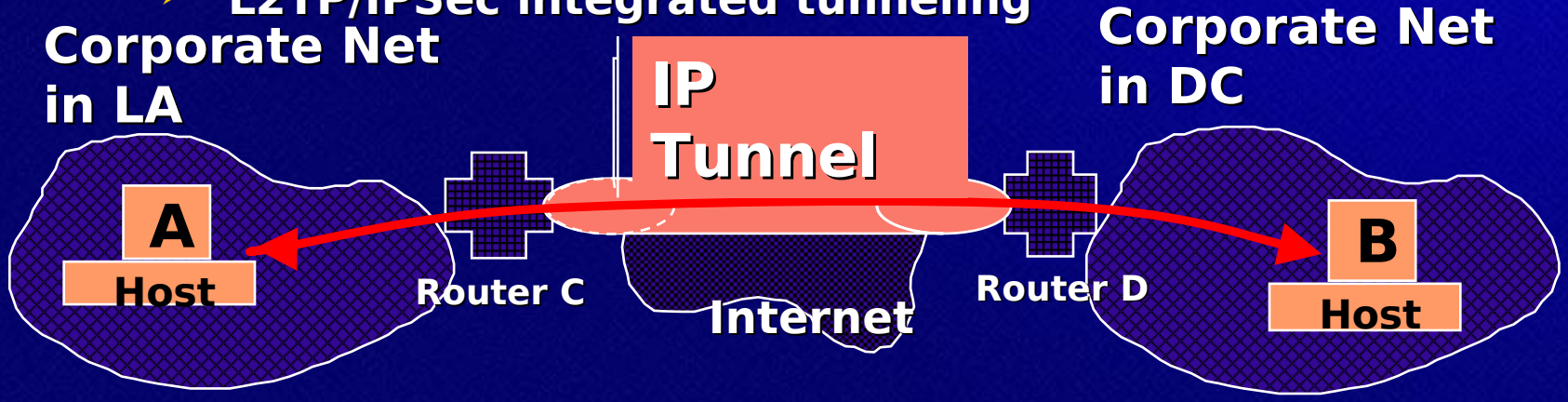
Windows 2000 IPSec
Target Scenarios

- Remote Access User to Corporate Network
  - Dial Up from Laptop or Home
  - Using existing network connectivity to Internet



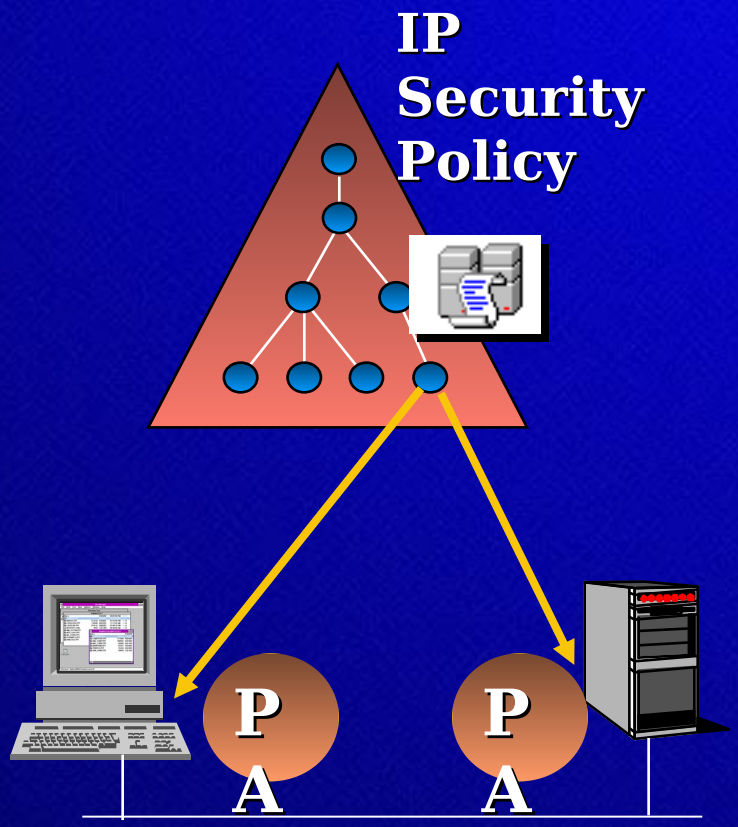
Windows 2000 IPSec Target Scenarios

- LAN Edge Gateway to Edge Gateway of Another LAN
  - Across Internet or private network with Windows 2000 <-> Windows 2000 routers using IP tunnels
    - IPSec Tunnel Mode
    - L2TP/IPSec integrated tunneling



IP Security

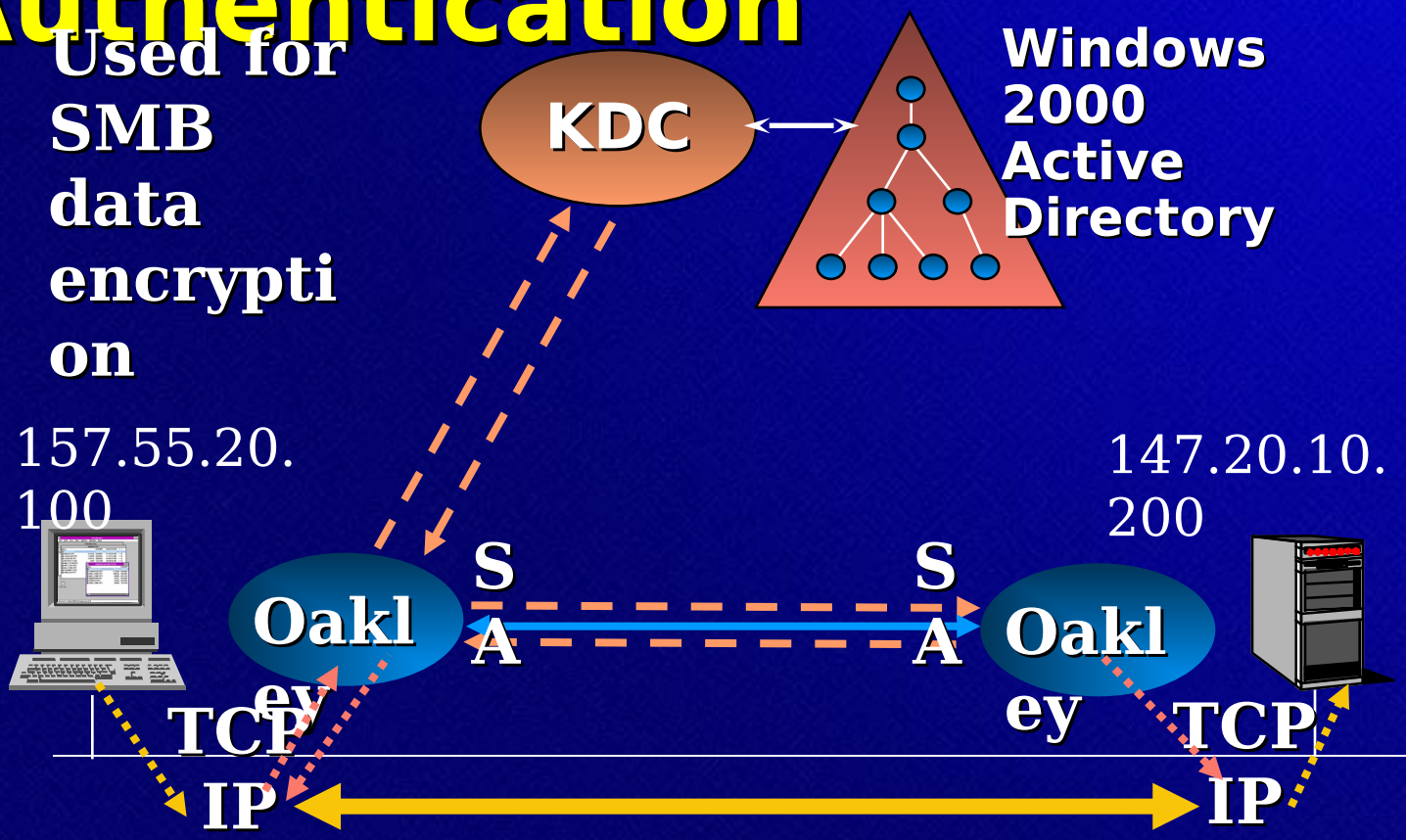
- Host-to-host authentication and encryption
  - Network layer
- IP security policy with domain policy
  - Negotiation policies, IP filters
- Policy Agent
  - Downloads IPSEC policy



Source:
157.55.00.00
Dest:
147.20.00.00

IP Security Association using Kerberos Authentication

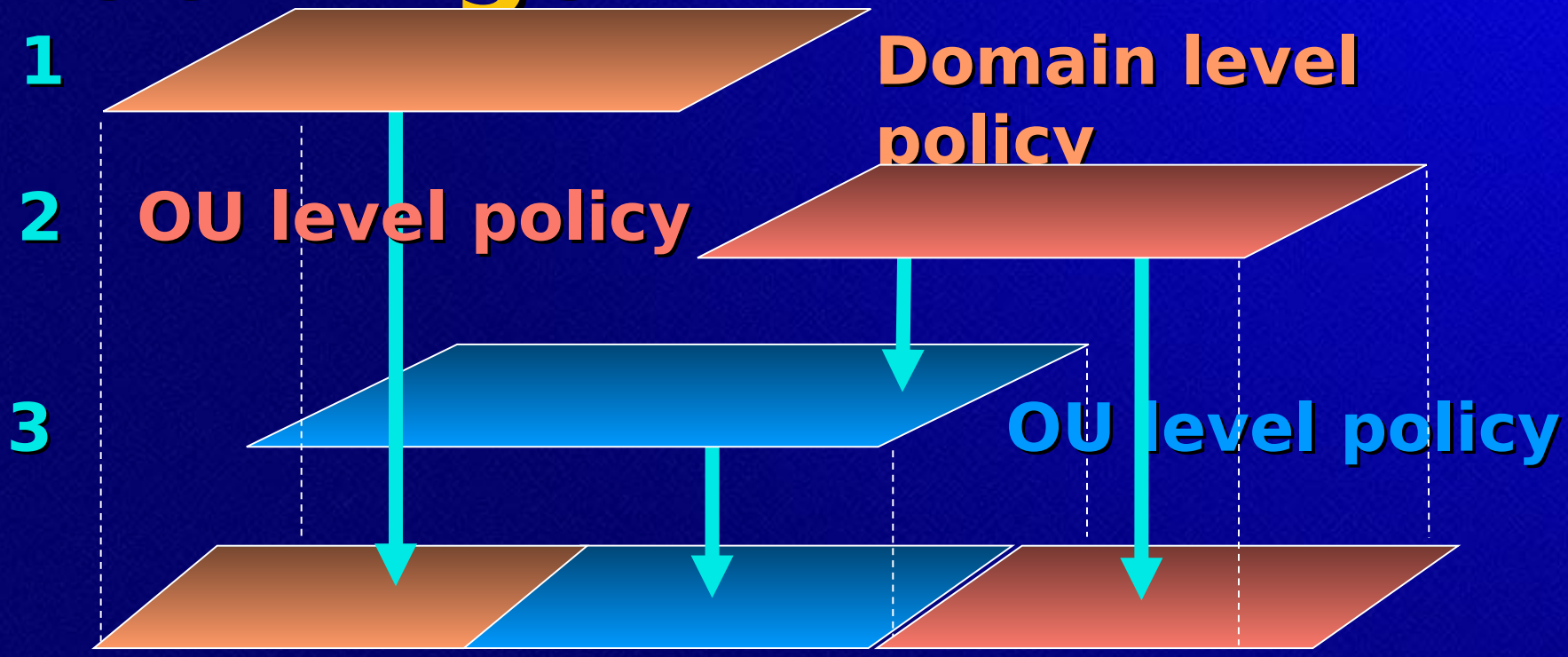
Used for SMB data encryption



Managing Security Policy

- Security settings in local or group policy
- Local computer policy
  - Audit policy, rights, security options
- Group Policy in the directory
  - Common computer policies
- Domain level policies
  - Account policies
  - Public key trust policies

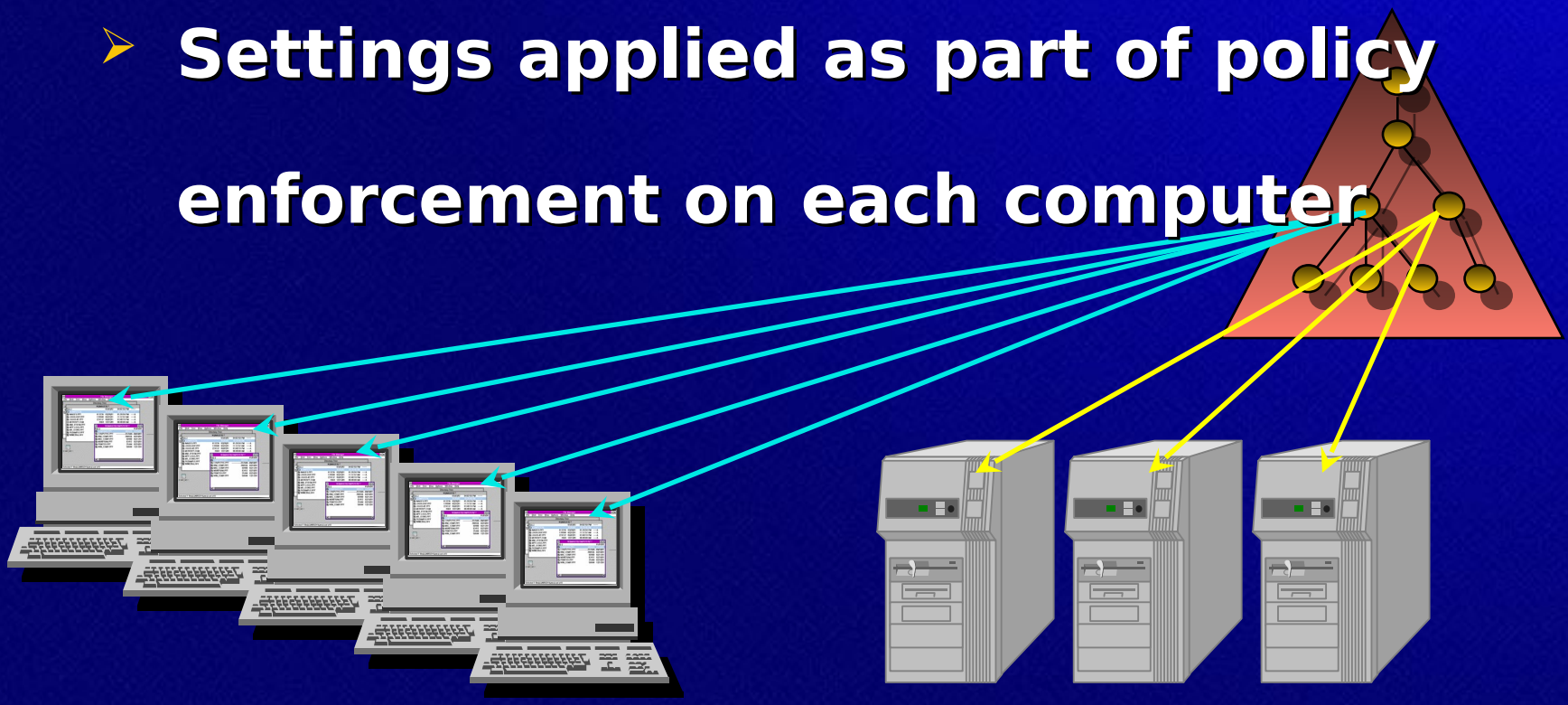
Hierarchical Policy Settings



- Applied policy for a computer combines multiple policy objects

Enterprise Framework

- Integrated with Group Policy management
  - Security settings in group policy
  - Settings applied as part of policy enforcement on each computer



For More Information

- Refer to the TechNet website at www.microsoft.com/technet/events/content

- Security Services White papers
  - http://www.microsoft.com/windows/server/deploy
- Windows 2000 Resource Kit
  - Multiple security chapters
- Microsoft Security Advisor
  - http://www.microsoft.com/security

Session Credits

- **Author:**
- **Producer/Editor:**
- **Thanks to Our Microsoft Technical Field personnel who reviewed this session:**
  - **Person 1**
  - **Person 2**
  - **Person 3**
  - **Person 4**
  - **Person 5**

Where do you want to go today?®

Microsoft®